



БОЛЬШИЕ ВЫЗОВЫ

ВСЕРОССИЙСКИЙ КОНКУРС
НАУЧНО-ТЕХНОЛОГИЧЕСКИХ ПРОЕКТОВ



Региональный трек
Всероссийского конкурса
научно-технологических проектов

«БОЛЬШИЕ ВЫЗОВЫ»

направление

Когнитивные исследования

название работы

Обучающая
программа «Асимметричная
криптосистема, основанная на
задаче «рюкзачка»

участник(и)

Капустин Владислав Игоревич

#большиевызовы
#МГК

г. Москва
2021

mgk.olimpiada.ru

Цель проекта:

создание достаточно простой и в то же время познавательной обучающей программы для эффективного изучения современных методов шифрования.

Задачи проекта:

- изучение всех компонентов информационной системы, в том числе и правовое обеспечение защиты информации, эксплуатации криптографических средств;
- разработка программного обеспечения;
- подготовка учебных материалов для проведения занятий по данной теме на основе кода программы.



Актуальность проекта:

Тема шифрования является наиболее популярной среди школьников разных возрастов. С каждым учебным годом рассматриваются все более и более сложные ее примеры, демонстрируя тем самым ее постоянную эволюцию.

Современное компьютерное шифрование использует последние достижения дискретной математики, алгебры, теории вероятностей, математической статистики, которые часто превышают уровень школьных знаний и являются предметом специального изучения в ВУЗах.

Поэтому создание обучающей программы, которая могла бы в доступной форме показать школьникам механизм шифрования, является весьма актуальной.

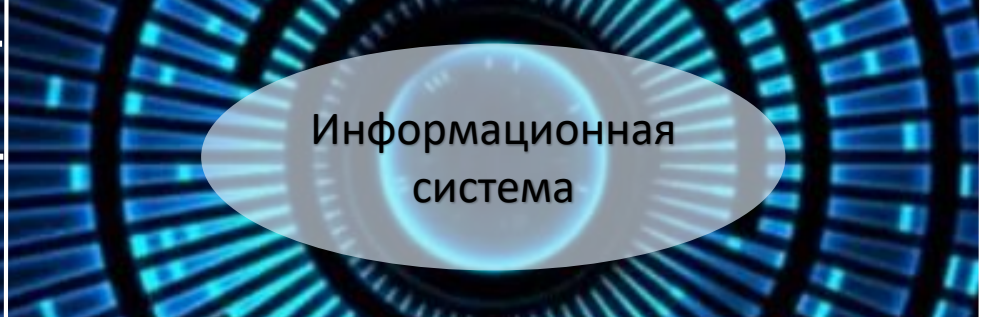


Дорожная карта проекта:

Направление работы, ключевые задачи \ Сроки	август 2020	сентябрь 2020	октябрь 2020	ноябрь 2020	декабрь 2020	январь 2021
Изучение методов шифрования, правовых основ защиты информации. Выбор метода шифрования, изучение математического аппарата.						
Анализ степени изученности и разработанности темы исследования. Постановка задач проекта.						
Разработка требований к обучающей программе. Выбор программной среды для реализации проекта.						
Разработка интерфейса и написание программного кода.						
Тестирование и модернизация программы.						
Подготовка учебных материалов на основе кода программы.						
Подготовка описания разработанного программного продукта и презентации для участия проекта в конкурсах.						

Входная информация

Для отправителя	Для получателя
<ul style="list-style-type: none">секретная информацияоткрытый ключ	<ul style="list-style-type: none">зашифрованное сообщениезакрытый ключ



Выходная информация

Для отправителя	Для получателя
<ul style="list-style-type: none">зашифрованное сообщение	<ul style="list-style-type: none">расшифрованное сообщение

Машинная реализация задачи

Аппаратное обеспечение	Программное обеспечение
<ul style="list-style-type: none">ЦПУ: 1 ГГц или вышеОЗУ: 512 МБ или выше	<ul style="list-style-type: none">Windows 7 / 8 / 10Python

Правовое обеспечение

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ
- Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Математическое обеспечение

- теоремы об общем наибольшем делителе двух чисел и мультипликативно обратном элементе
- расчет открытого ключа:
 $n_1 = (W * n_1^s) \bmod M$
- формула зашифровки сообщения:
 $C_i = n_1 * x_{(i-1)k+1} + n_2 * x_{(i-1)k+2} + \dots + n_k * x_{ik}$
- формулы шифра Виженера:
 $C_i = (P_i + K_i) \bmod M$
 $P_i = (C_i - K_i + M) \bmod M$
- формула для дешифровки:
 $C_i^s = (W^{-1} * c_i) \bmod M$

Введите элементы супервозрастающей последовательности
или нажмите кнопку **RANDOM**



Первый элемент

Второй элемент

Третий элемент

Четвертый элемент

Пятый элемент

Шестой элемент

Седьмой элемент

Восьмой элемент

Введите кодовое число M
превышающее сумму всех элементов



Рассчитать открытый ключ

Полученное число W

взаимно простое с M

Найденное число iW

мультипликативно обратное к W

Сохранить открытый ключ

Сохранить закрытый ключ

Введите открытый ключ

1123 2114 595 926 245 2824 2587 969

Введите сообщение

Пример секретного сообщения

Зашифрованное сообщение

4946 2366 8631 8630 2249 8759 8098 4786 7495
4907 2327 5036 2693 5647 480 86 4009 3348 36
3959 7882 4901 2270 4979 7933 5108 2485 9089

Загрузить из файла

Зашифровать сообщение

Сохранить шифровку

Шифрование завершено!

2485 5108 7933 4979 2270 4901 7882
3959 36 3348 4009 86 480 5647 2693
5036 2327 4907 7495 4786 8098 8759
2249 8630 8631 2366 4946 6467 6265
2954 2709 6459 6109 3923 3923 5778
8429 3923 8696 3923 2954 6747 2709
6510 6502 2709 5778 8429 6510 2709
9089 6265 6510 4946 ['0', '1', '0', '0', '1',
'0', '1', '0'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0',
'1', '1', '0', '0', '0', '1', '1'] ['0', '1', '1', '0', '0',
'1', '1', '1'] ['0', '1', '1', '0', '0', '0', '0', '0'] ['0',
'1', '1', '0', '1', '0', '1', '1'] ['1', '0', '0', '1', '0',
'1', '1', '1'] ['0', '1', '1', '0', '1', '1', '0', '0'] ['0',
'1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '0',
'1', '0', '1'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0',
'1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1',
'1', '0', '1'] ['0', '1', '1', '0', '1', '0', '0', '0'] ['0',
'1', '1', '0', '1', '0', '0', '1'] ['0', '1', '0', '1', '1',
'1', '1', '0'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['1',
'0', '0', '1', '0', '1', '1', '1'] ['0', '1', '1', '0', '1',
'1', '0', '0'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['0',
'1', '1', '0', '1', '0', '0', '1'] ['0', '1', '0', '1', '1',
'1', '0', '0'] ['0', '1', '1', '1', '0', '1', '0', '0'] ['0',
'1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1',
'0', '0', '0'] ['0', '1', '1', '0', '0', '0', '1', '1'] ['0',

Введите закрытый ключ

5 19 41 100 228 460 884 1810 3589 2378 1876

Введите зашифрованное сообщение

4946 2366 8631 8630 2249 8759 8098 4786 7495
4907 2327 5036 2693 5647 480 86 4009 3348 36
3959 7882 4901 2270 4979 7933 5108 2485 9089

Расшифрованное сообщение

Пример секретного сообщения

Загрузить из файла

Загрузить из файла

Расшифровать сообщение

Сохранить сообщение

Расшифровка завершена!

```
янешбоос огонтеркес ремирП['0', '1',  
'1', '1', '1', '0', '1', '0'] ['0', '1', '1', '0', '0', '0',  
'1', '1'] ['0', '1', '1', '0', '1', '0', '0', '0'] ['0', '1',  
'1', '0', '0', '0', '0', '0'] ['0', '1', '1', '1', '0', '1',  
'0', '0'] ['0', '1', '0', '1', '1', '1', '0', '0'] ['0', '1',  
'1', '0', '1', '0', '0', '1'] ['0', '1', '1', '0', '1', '0',  
'0', '1'] ['0', '1', '1', '0', '1', '1', '0', '0'] ['1', '0',  
'0', '1', '0', '1', '1', '1'] ['0', '1', '1', '0', '1', '0',  
'0', '1'] ['0', '1', '0', '1', '1', '1', '1', '0'] ['0', '1',  
'1', '0', '1', '0', '0', '1'] ['0', '1', '1', '0', '1', '0',  
'0', '0'] ['0', '1', '1', '0', '1', '1', '0', '1'] ['0', '1',  
'1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1', '0',  
'1', '1'] ['0', '1', '1', '0', '0', '1', '0', '1'] ['0', '1',  
'1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1', '1',  
'0', '0'] ['1', '0', '0', '1', '0', '1', '1', '1'] ['0', '1',  
'1', '0', '1', '0', '1', '1'] ['0', '1', '1', '0', '0', '0',  
'0', '0'] ['0', '1', '1', '0', '0', '1', '1', '1'] ['0', '1',  
'1', '0', '0', '0', '1', '1'] ['0', '1', '1', '0', '1', '0',  
'1', '1'] ['0', '1', '0', '0', '1', '0', '1', '0'] 1272  
2754 288 60 620 807 2098 2098 748  
3259 2098 1691 2098 288 2558 60 2982  
2330 60 748 3259 2982 60 3214 2754  
2982 1131 4946 6510 6265 9089 2709  
6510 8429 5778 2709 6502 6510 2709  
6747 2954 3923 8696 3923 8429 5778
```



Подготовка учебных материалов на основе кода программы

Основные классы

Модуль tkinter включает следующие классы:

1. **Button** (кнопка)
2. **Radiobutton** (радио-кнопка)
3. **Checkbutton** (флажок)
4. **Entry** (однострочное поле для ввода)
5. **Text** (многострочное поле для ввода)
6. **Label** (метка)
7. **Scale** (ползунок)
8. **Scrollbar** (полоса прокрутки)
9. **Frame** (виджет для группировки других виджетов)
10. **LabelFrame** (аналог Frame, только с заголовком)
11. **Listbox** (список)
12. **Canvas** (поле для рисования)
13. **PanedWindow** (элемент разделения окна)
14. **Menu** (главное меню)
15. **Tk** (главное единственное окно)
16. **Toplevel** (дочернее окно)

Button

Виджет Button - самая обыкновенная кнопка, которая используется в тысячах программ. Пример кода:

```
from Tkinter import *
root=Tk()
button1=Button(root,text='ok',width=25,height=5,bg='black',fg='red',font='arial 14')
button1.pack()
root.mainloop()
```

Разберем этот небольшой код. За создание собственно окна отвечает класс Tk() и первым делом нужно создать экземпляр этого класса. Этот экземпляр вы можете назвать его как угодно.

- text - какой текст будет на кнопке.
- width,height - соответствующие размеры кнопки.
- bg - цвет кнопки (свойство цвета фона).
- fg - цвет текста на кнопке.
- font - шрифт и его размер.

Далее, нашу кнопку необходимо разместить в окне. Пока, чтобы разместить кнопку в окне не будет создано

Label

Label - это виджет, предназначенный для отображения какой-либо надписи без возможности редактирования пользователем. Имеет те же свойства, что и Button.

Entry

Entry - это виджет, позволяющий пользователю ввести одну строку текста.

- **borderwidth** - ширина бордюра элемента
- **bd** - сокращение от **borderwidth**
- **width** - задаёт длину элемента в знаках.
- **show** - задает отображаемый символ.

Text

Text - это виджет, который позволяет пользователю ввести любое количество текста. Имеет дополнительное свойство wrap, отвечающее за перенос слов, нужно использовать значение WORD. Например:

```
from Tkinter import *
root=Tk()
text1=Text(root,height=7,width=7,font='Arial 14',wrap=WORD)
text1.pack()
root.mainloop()
```

```
main.py [C:\Users\garry\AppData\Local\Temp\main.py] - D:\Информатика\Pascal-Python\Tkinter\Project\tab2.py - PyCharm
File Edit View Navigate Code Refactor Run Tools VCS Window Help
D:\Информатика\Pascal-Python\Tkinter\Project\tab2.py
Project main.py bin_code.py tab1.py tab2.py tab3.py tab4.py tab5.py
main.py
External Libraries
Scratches and Consoles
182 else:
183     messagebox.showinfo('Message', "Ошибка в 2 элементе")
184
185 m = int(self.M.get())
186 w = random.randint(2, m)
187 while self.nod(w, m) != 1:
188     w = random.randint(2, m)
189 self.W.configure(state='normal')
190 self.W.delete(0, END)
191 self.W.insert(0, w)
192 self.W.configure(state='disabled')
193 self.W2.configure(state='normal')
194 self.W2.delete(0, END)
195 self.W2.insert(0, w)
196 self.W2.configure(state='disabled')
197 iw = m - 1
198 while (w * iw) % m != 1:
199     iw -= 1
200 self.iw.configure(state='normal')
201 self.iw.delete(0, END)
202 self.iw.insert(0, iw)
203 self.iw.configure(state='disabled')
204
205 n1 = (w * int(self.ns1.get())) % m
206 n2 = (w * int(self.ns2.get())) % m
207 n3 = (w * int(self.ns3.get())) % m
208 n4 = (w * int(self.ns4.get())) % m
209 n5 = (w * int(self.ns5.get())) % m
210 n6 = (w * int(self.ns6.get())) % m
211 n7 = (w * int(self.ns7.get())) % m
212 n8 = (w * int(self.ns8.get())) % m
213 # self.N.configure(state='normal')
214 self.N.delete(0, END)
215 self.N.insert(0, "{} {} {} {} {} {} {} {}".format(n1, n2, n3, n4, n5, n6, n7, n8))
216 # self.N.configure(state='disabled')
217 self.N.bind("<Button-3>", self.k_menu)
218
```

Результат проекта:

Разработанное программное обеспечение может выступать в роли дополнительного учебного материала по теме информационной безопасности, а также в рамках изучения создания графических приложений.

Создание таких обучающих программ становится особенно актуальным в связи с проведением в 2020 - 2022 годах эксперимента по внедрению целевой модели цифровой образовательной среды.

Таким образом, цель данного проекта созвучна с теми приоритетными задачами, которые поставлены перед школой в настоящее время – повышение доступности качественного образования.

Дальнейшее развитие проекта:

- ✓ создание веб-версии программы для размещения ее в открытом доступе;
- ✓ создание англоязычной версии для расширения аудитории сайта;
- ✓ размещение обучающей программы в виде приложения в МЭШ;
- ✓ информационная методическая поддержка (проведение вебинаров, запись обучающих видеороликов)

